CLAIMS

1. A method of creating an http client authentication object, comprising:

a) requesting an http file on an http server;

b) retrieving conforming client data;

c) inputting said conforming client data into a http client authentication object;

d) transmitting the http client authentication object; and

e) storing the http client authentication object in a storage means on an http client computer means.

2. A method of claim 1, wherein the conforming client data is retrieved from the http client or a storage means on which client data is stored.

3. A method of claim 1, wherein the conforming client data is the client's IP address or password.

4. A method of claim 3, further comprising encrypting the client password before inputting the password into the client authentication object.

5. A method of claim 3, further comprising hashing the client password prior to inputting.

6. A method of claim 1, wherein the conforming client data is a Kerberos ticket.

7. A method of claim 1, wherein the conforming client data is a digital signature of the http client on the time-stamp and the inputting is by the client or the http server.

8. A method of claim 1, further comprising: encrypting the conforming client data after b) retrieving conforming client data from the http client.

9. A method of claim 1, further comprising: encrypting the conforming client data using a public-key provided by the http server, wherein said encrypting is performed after b) retrieving conforming client data from the http client.

10. A method of claim 8, wherein the encrypted conforming client data can be decrypted by the http server using a private-key.

11. A method of claim 1, further comprising: encrypting the conforming client data using a secret-key, wherein said encrypting is performed after b) retrieving conforming client data from the http client.

12. A method of claim 11, wherein the encrypted conforming client data can be decrypted by the http server using a secret-key.

13. A method of creating an http confidential object, comprising:

a) obtaining client data;

b) encrypting the client data to formed encrypted client data; and

c) inputting the encrypted client data into a http confidential object.

14. A method of claim 13, wherein the client data is credit card data, social security number, or a home address.

15. A method of claim 13, wherein the encrypting b) is accomplished using a public-key provided by the http server.

16. A method of claim 13, wherein the encrypted data can be decrypted by the http server using a private-key.

17. A method of claim 13, wherein the encrypting b) is accomplished using a secret-key.

18. A method of claim 17, wherein the encrypted data can be decrypted by the http server using a secret-key.

19. A method of authenticating an http client accessing an http server, comprising:

a) retrieving an authentication object from an http client;

b) comparing the retrieved authentication object with conforming client data to determine whether retrieved authentication object contains the same conforming client data.

20. A method of claim 19, wherein the conforming client data is the client's IP address, password, Kerberos ticket, or digital signature of the client.

21. A method of claim 19, whereby comparing the retrieved authentication object is decrypting encrypted conforming client data and determining whether the decrypted conforming client data is the same conforming client data inputted by the client in that same session or is the same conforming data retrieved by the http server in that session.

22. A method of claim 19, wherein the authentication object contains a digital signature of the http client on the time-stamp.

23. A method of claim 22, whereby comparing the retrieved authentication object is verifying the digital signature using a public-key and determining whether the digital signature is the http client's digital signature.

24. A method of providing integrity to client objects transmitted to an http server from an http client comprising:

a) creating integrity data from one or more http client objects;

b) inputting the integrity data into a http client integrity object; and

c) storing the http client integrity object.

25. A method of claim 24, wherein: the integrity data is created by public-key based cryptography of the one or more http client objects.

26. A method of claim 25, wherein the public-key based cryptography is a digital signature of the http server on a message digest of the one or more http client objects.

27. A method of claim 24, wherein: the integrity data is a created by secret-key based cryptography of the one or more http client objects.

28. A method of claim 27, wherein, the secret-key based cryptography is keyed-message digest or HMAC.

29. A method of claim 24, wherein the http client objects are a http client authentication object and a client object comprising client data.

30. A set of secure client objects, comprising:

a) a client object comprising client data

b) a client authentication object; and

c) a client integrity object.

31. A set of secure objects of claim 30, wherein the objects are the objects set forth in Fig. 4.

32. A method of performing an electronic transaction on the Web, comprising: retrieving a set of secure client objects of claim 30.

33. A method of claim 32, wherein the electronic transaction is an authentication service, electronic commerce, pay-per-access, or attribute-based access control.

34. A client system for storage and transfer of secure data on the Web, comprising: a computer means for requesting a file from a server; a means for receiving secure client objects; and a storage means, the storage means comprising: a client authentication object.

35. A client system of claim 34, wherein the storage means further comprises a client authentication object and a client integrity object.

36. A client system of claim 34, wherein the means for requesting a file from a server is an executable program.

37. A server system for storage and transfer of secure data on the Web, comprising: a file request means for receiving a file request from a client; a client object means for receiving client data and storing client data as a client object; and a transfer means for transferring a client object to a client system.

38. A server system of claim 37, wherein the client object means further comprises a means for inputting a client integrity object.

39. A system for storage and transfer of secure data on the Web, comprising: a means for receiving, storing, transferring, or inputting:

a) a client object comprising client data

b) a client authentication object; or

c) a client integrity object.